TL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/874,292	06/06/2001	Gary Manuel Jackson	63795-0007	6320

24633 7590 02/10/2006

HOGAN & HARTSON LLP
IP GROUP, COLUMBIA SQUARE
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/874,292	JACKSON, GARY MANUEL	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,11-14,17,18,25 and 30-33* is/are rejected.

7)☒ Claim(s) *2-10,15,16,19-24 and 26-29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/25/2005 has been entered.

Response to Amendment

2. As per Applicant's arguments in regards to Joyce, the Applicant's Arguments were persuasive. The prior art has been changed to rejected claims. Thus, the Applicant's remarks in regards to Joyce are moot.

Allowable Subject Matter

3. Claims 2-10, 15-16, 19-24, and 26-29 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an

international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 11-14, 17-18, 25, 30-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Lyle et al(6,971,028).

5. As per claims 1, 30-31, Lyle et al. discloses a method for detecting unauthorized intrusion in a network system(see col. 2, lines 59-60), receiving packet level activity information from the network(see col. 2, lines 47-50, col. 10, lines 38-43); collecting sequential samples of sorted port specific activity information from the received packet level activity information for each IP/user(see col. 7, lines 3-16), converting packet level activity into human behaviors and activities for each IP/user(see col. 7, lines 32-38, 43-50), converting the sorted IP/user behavioral activities into behavioral measures of expertise and deception as measures of underlying intent for each IP/user(see col. 7, lines 43-61), monitoring sequential determinations of the converted human intent behavioral measures, for the duration that each IP/user is in the network(see col. 8, lines 34-53); wherein the monitoring step includes determining new and previously undetected misuse behaviors as indicated by increased intent levels of expertise and deception(see col. 14, lines 3-20); passive gathering of tracked intent information for any given IP/user if monitored expertise and deception measures exceed intent thresholds underlying non-misuse network activity(see col. 10, lines 38-53).

6. As per claims 11, 25, Lyle et al. discloses wherein the tracking action includes storing activity information in a tracking module(see col.7, lines 13-16).

7. As per claim 12, Lyle discloses a traffic sorter that receives a copy of the network activity and sorts such all activities by IP/user for the purpose collecting sequential samples of each

IP/user's activities/behaviors by IP/users(see col. 7, lines 3-12); an activity monitor operatively coupled to the traffic sorter for sequentially monitoring converted human intent behaviors and activities by IP/users(see col. 7, lines 43-58); an inter-port fusion module that fuses assessments from one or more assessment engines that monitor behavior measures by port and non-port specific behavior conversions(see col. 7, lines 43-58); and an outcome director operatively coupled to the inter-port fusion monitor(see col. 8, lines 6-14).

8. As per claim 13, Lyle discloses wherein the activity monitor includes at least one dedicated port monitor(see col. 7, lines 32-58).

9. As per claim 14, Lyle discloses wherein, the at least one dedicated port monitor includes a packet level analysis module, an activity translator module and an assessment module(see col.7, lines 32-64).

10. As per claim 17, Joyce discloses wherein the traffic sorter receives packet level activity information from the network and sorts the port specific activity information from the network into IP users(see col. 7, lines 3-12).

11. As per claim 18, Joyce discloses wherein the activity monitor monitors the port specific activity information (see col. 7, lines 32-58).

12. As per claim 32, Lyle discloses wherein the step of receiving the port specific activity information includes creating a copy of the network activity sorted by users(see col. 8, lines 45-53).

13. As per claim 33, Lyle discloses the step of sorting non-port specific activity information from the received packet level activity information by the IP/user; and converting the non-port

specific activity information to human behavioral measures of intent(see col. 7, lines 32-38, 43-50).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

February 4, 2006

Jenise E. Jackson

2/6/06